

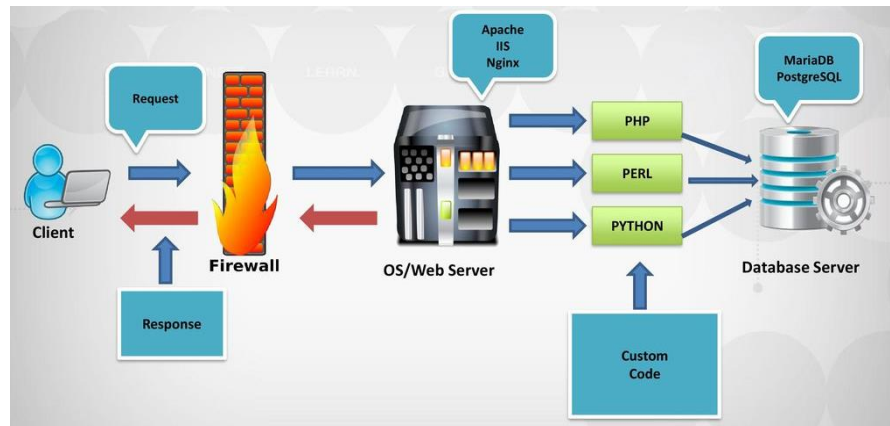
FSI LEI 2025/2026

Practical class #7

- **Web application security with OWASP ZAP and Kali**

Web Application Security

- Web application security is a central component of any web-based business
- Web applications expose web properties to attack from different locations and various levels of scale and complexity
- Web application security deals with the security surrounding websites, web applications and web services



Main Web Application Security Risks (1)

- Cross-Site Scripting XSS
 - XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- Injection
 - Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- Broken Authentication
 - Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- Broken Access Control
 - Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Main Web Application Security Risks (2)

- Sensitive Data Exposure

- Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

- Security Misconfiguration

- Security misconfiguration is the most commonly seen issue, commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

- Using Components with Known Vulnerabilities

- Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

- Insecure Deserialization

- Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.



- The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software
- Highlights:
 - Community-led open source software projects
 - Over 275 local chapters worldwide
 - Tens of thousands of members
 - Industry-leading educational and training conferences
- Open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted
- All projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security

Web Security Testing Guide (WSTG) Project

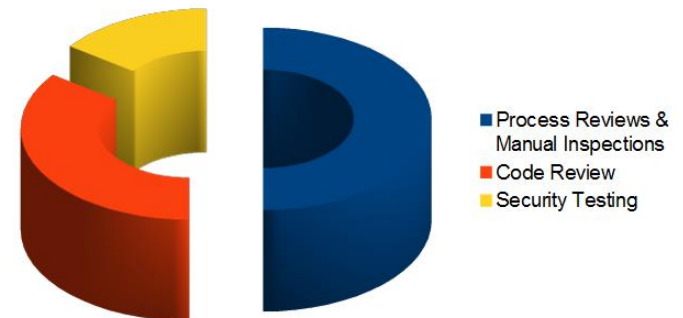
- The WSTG is a comprehensive guide to testing the security of web applications and web services
- Created by the collaborative efforts of security professionals and dedicated volunteers
- WSTG provides a framework of best practices used by penetration testers and organizations all over the world

<https://github.com/OWASP/wstg/tree/master/document>

WSTG Project

4. Web Application Penetration Testing

- 4.1 Information Gathering
- 4.2 Configuration and Deployment Management Testing
- 4.3 Identity Management Testing
- 4.4 Authentication Testing
- 4.5 Authorization Testing
- 4.6 Session Management Testing
- 4.7 Input Validation Testing
- 4.8 Error Handling
- 4.9 Cryptography
- 4.10 Business Logic Testing
- 4.11 Client Side Testing



Security approaches

- Black box testing
 - Tools such as Web application security scanners, vulnerability scanners and penetration testing software
- White box testing
 - Tools such as static source code analyzers
- Fuzzing
 - Tools used for input testing
- Web application security scanner
 - Vulnerability scanner
- Web application firewalls (WAF)
 - Used to provide firewall-type protection at the web application layer
- Password cracking tools
 - For testing password strength and implementation

Black-Box Testing Tools

Some examples

- General Testing
 - **OWASP ZAP**
 - Burp Proxy
 - Webstretch Proxy
 - W3af
 - Subgraph Vega
- Commercial
 - NGS Typhon
 - IBM AppScan
 - Burp Intruder
 - Acunetix Web Vulnerability Scanner
 - MaxPatrol Security Scanner
 - Parasoft SOAtest (more QA-type tool)
 - N-Stalker Web Application Security Scanner
 - SoapUI (Web Service security testing)
 - Netsparker
 - SAINT
 - QualysGuard WAS
 - IndusGuard Web
- Linux Distribution
 - PenTestBox
 - Samurai
 - Santoku
 - ParrotSecurity
 - **Kali**
 - Matriux
 - BlackArch
 - PenToo
- Source Code Analyzers
 - Spotbugs
 - Find Security Bugs
 - FlawFinder
 - phpcs-security-audit
 - PMD
 - Microsoft's FxCop
 - Oedipus
 - Splint
 - SonarQube
 - W3af

OWASP ZAP

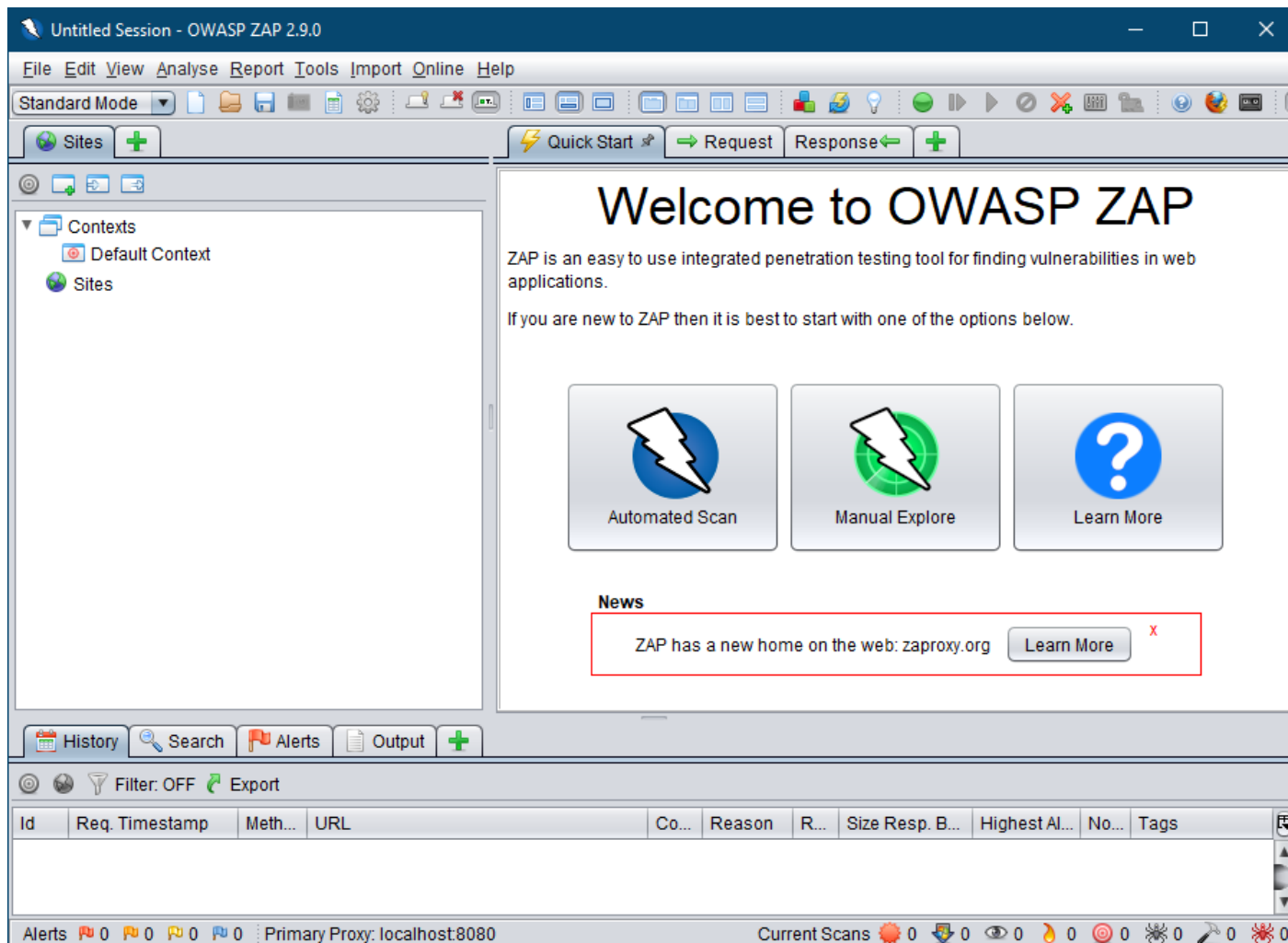


- Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool
- Maintained under the umbrella of the OWASP
- ZAP is designed specifically for testing web applications
- ZAP is a man-in-the-middle proxy
 - ZAP stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination



<https://www.zaproxy.org/>

OWASP ZAP



Kali Linux



- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing
- Kali contains several hundred tools which are geared towards various information security tasks, such as:
 - Penetration Testing
 - Security research
 - Computer Forensics
 - Reverse Engineering
- Kali Linux is an open source project that is specifically tailored to the needs of penetration testing professionals

<https://www.kali.org/>

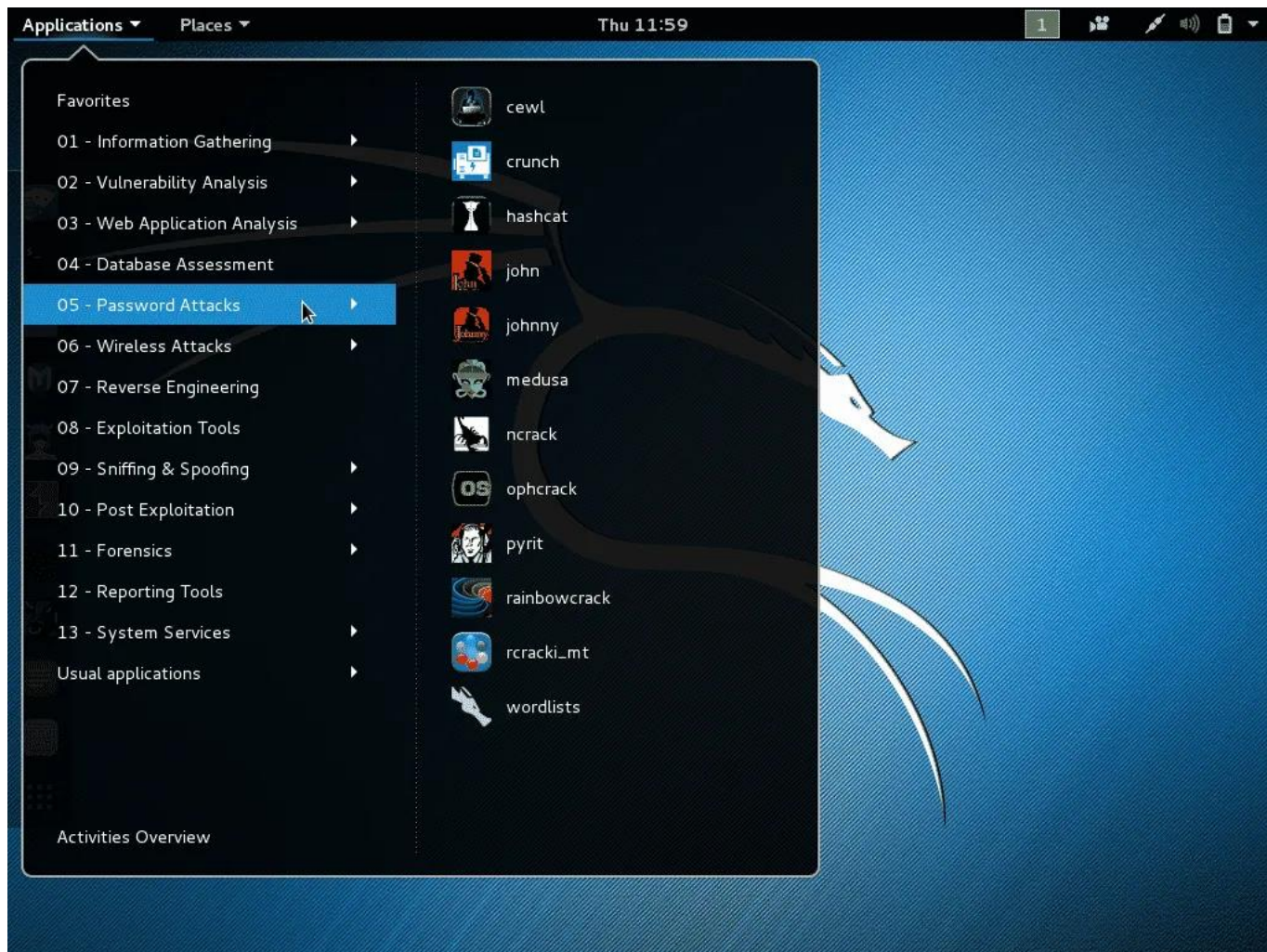
STARTING THE EXERCISE

Exercise with OWASP ZAP

- Install OWASP ZAP:
 - <https://www.zaproxy.org/download/>
- To start testing use: Automated Scan
- More information is available at:
 - <https://www.zaproxy.org/getting-started/>
- Analyse results and conduct exploitation of identified threats





























Exercise with Kali Linux



Exercise with Kali

- Install Kali (in a VM):
 - <https://www.kali.org/get-kali/#kali-virtual-machines>
- To start testing use tools available in the [kali-tools-web](#) package
- Use the documentation for each tools ([kali tools](#))
 - [burpsuite](#)
 - [wpscan](#)
 - [wapiti](#)

 apache-users
 burpsuite
 cutycapt
 dirb
 eyewitness
 heartleech
 hydra
 joomscan
 lbd
 mitmproxy
 nishang
 owasp-mantra-ff
 patator
 plecost
 qsslaudit
 siege
 sqldict
 sqlninja
 sslh
 sslsplit
 thc-ssl-dos
 uniscan
 watobo
 webshells
 whatweb
 xsser

 apache2
 cadaver
 davtest
 dirbuster
 ftester
 httpprint
 hydra-gtk
 jsq1-injection
 maltego
 ncrack
 nmap
 padbuster
 php
 proxychains4
 redsocks
 skipfish
 sqlitebrowser
 sqlsus
 sslscan
 sslyze
 tlssled
 wafw00f
 webacoo
 weevely
 wireshark
 zaproxy




 beef-xss
 commix
 default-mysql-server
 dotdotpwn
 hamster-sidejack
 httrack
 jboss-autopwn
 laudanum
 medusa
 nikto
 oscanner
 paros
 php-mysql
 proxytunnel
 sidguesser
 slowhttptest
 sqlmap
 ssldump
 sslsniff
 stunnel4
 tnscomd10g
 wapiti
 webscarab
 wfuzz
 wpscan

Altoro Mutual (demo site)

← → ↻ ⚠ Not Secure | demo.testfire.net

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none">• Deposit Products• Lending Services• Cards• Insurance• Retirement• Other Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none">• About Us• Contact Us• Locations• Investor Relations• Press Room• Careers• Subscribe	<p>Online Banking with FREE Online Bill Pay</p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p>  <p>Real Estate Financing</p> <p>Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.</p>	 <p>Business Credit Cards</p> <p>You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.</p> <p>Retirement Solutions</p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p>Privacy and Security</p> <p>The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.</p>  <p>Win a Samsung Galaxy S10 smartphone</p> <p>Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.</p>

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro Mutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.